CYBER INSURANCE – A PRIMER

Table of Contents

Welcome to SeedPod Cyber

SeedPod is the first cyber insurance platform that leverages the partnership between Managed Service Providers and small and medium sized businesses to assess, mitigate and transfer risk so all can safely compete and thrive in this digital world.

In this paper, “Cyber Insurance: A Primer”, we will be taking a deep dive into cyber insurance, what carriers expect, and what businesses need to know.

What is cyber insurance?

Cyber insurance protects your organization in the event of a cyber-attack. In many cases, it can cover the cost of liability when you are sued by your customers or others. It can also cover the costs associated with getting your systems back to where they were before the cyber event occurred. In certain situations, it will cover you for lost income that is sustained while your system has been down.

Isn't this insurance included in other policies?

In fact, there is a lot of gray area in what is covered and not covered between your general liability and property coverages versus cyber insurance coverage. Many carriers are explicitly excluding acts relating to cyber risks from their property and general liability coverages.
In almost all cases, many of the first party coverages found in a cyber insurance policy would not be found in either a property or general liability policy. So, if you do feel you have risks relating to cyber, you should be thinking about having a standalone cyber insurance program in place.

What are the various components typically found in a cyber insurance policy?

There are two basic categories of coverage; one is third party and the second is first party.

Third Party Coverage
Third party coverage is liability coverage. In other words, it protects you from a third party making a claim against you. As an example, if you have a data breach in which your customers records are taken, your customer may sue you for damages. There is also a liability for media and content, which provides coverage in the event there is something on your website that misrepresents or infringes on copyright or is an invasion of privacy and are sued. Then there are

typically liabilities around regulatory fines, penalties, and defense that may arise given the privacy and cyber laws that exist and will continue to grow over time.

First Party Coverage

First Party Coverage provides coverage for costs you have in the event of a cyber incident. Most cyber insurance claims have been, historically, first party claims.

Notification Costs

A usual first party coverage would be to cover breach notification costs; the costs you must pay to provide notification and perhaps credit monitoring services to clients who may have been impacted by a covered data breach. These costs usually include a breach coach (often an attorney) who guides you through the process to determine what your obligations are with regards to notification. Additionally, these costs typically include forensics to identify the source and scope of the breach.

Systems Restoration

Another component that many policies include is systems restoration, which are costs to get your system back to the way it was prior to the breach. Additional coverages associated with systems restoration is **data recovery** (which covers the costs of getting data back on your system) and **bricking**, which covers the costs for computers and hardware that are damaged beyond repair.

Ransomware

Another key coverage is for ransomware. Ransomware is a type of cybersecurity incident where the hacker encrypts your data and requires you to pay them a ransom (typically in bitcoin) to get the encryption code "keys" to regain access. Historically, cyber insurance covers both the costs to restore your systems as well as the ransomware payment itself. However, given the dramatic increase in ransomware over the past 18 months, that is beginning to change (see below).

Business Income

In addition, many policies include some form of Business Interruption Coverage which is often triggered to cover the costs of lost profit that may occur while systems are down due to a covered event. Say you suffer a ransomware attack, the average downtime for an organization is approximately three weeks. That is three weeks in which you could be suffering from lost profit, either as the result of having to increase your staff to cover the fact that your systems are not online, to pay additional personnel that are not covered by insurance to help get your systems back up, or to account for lost revenues, profit from lost revenues, and the fact that you are unable to sell or retain your clients during that period of time. That is where business interruption comes in, and that has been a major area in which carriers have seen a lot of claims activity, especially when it comes to ransomware attacks.

There is a variant of business income, called **contingent business income**, that covers the loss of profits due to an interruption of 3rd party computer services or software. You must read your coverage carefully, but as an example, if you had your data stored in the cloud and the cloud provider went down and you lost access to your data, this coverage could be triggered.

Cyber Crime

Cyber Crime is another category of first party expenses that focuses on acts of Fraud. **Computer Fraud** covers funds or property that are stolen because of a hacking exploit. **Funds Transfer Fraud** covers funds involved when a hacker induces a bank or financial institution to transfer funds to a fraudulent account. **Social Engineering** coverage pays when hackers induce someone to transfer funds willingly. As an example, the account department agrees to wire money upon receipt on an email from the CEO, when in fact, it was not the CEO, but a hacker impersonating (or "spoofing") one. Some carriers also provide coverage for **Invoice Manipulation** (when a hacker fraudulently changes the invoices to customers), **Telecommunications Fraud** (when a hacker uses your telephone plans for their communication purposes) or **Crypto-Jacking** (when a hacker gains control of your system for the purpose of crypto-mining).

Other Coverages

Cyber Insurance is continually changing and its coverages evolving. Additional coverages include reputational harm coverage, crisis management coverage and privacy regulation coverage (which is becoming more important as states adopt privacy regulations).

The problem with ransomware

As noted, ransomware has exploded over the past 18 to 24 months, due largely to the impact of working from home. This has resulted in significant losses, and carriers are looking for ways to limit their exposure. Many carriers are imposing sub-limits on how much ransomware extortion coverage they will provide. Other carriers are excluding the ransom payment from their coverage altogether.

Many carriers and other individuals in the cybersecurity space have asked whether cyber insurance has contributed to the explosion. Afterall, so they say, if there is coverage for the ransom demand, won't that incent bad guys to ask for it?

It is an interesting question and two sides to the argument. The one side is we do not want to incent bad guys to continue to hack us with ransomware attacks. The other side of the argument is if a business, hospital, or public utility has a ransomware attack and they are unable to restore their systems without paying the ransom, they could be out of business forever. Not to mention, it could impact patient treatment or seriously harm infrastructure or

supply chains. While there is no concrete resolution, it pays you to pay particular attention to how your carrier is treating ransomware.

What are the factors to consider when deciding what and how much coverage to get?

There is no strict rule of thumb on how much insurance you should buy but here are a couple of things that you should be considering. One is **what type of data** do you have? Do you have sensitive data? Whether it is financial or healthcare data, confidential information on your own intellectual property, or confidential or patient information that is held on behalf of your clients. That is going to impact how much coverage you should get.

Another factor is **how much data** you have. If you are dealing with thousands of customers, you are going to need a lot more coverage than if you are dealing with hundreds of customers, for the most part. It depends on who those customers are and what the negative impact could be if their data was breached, stolen, or rendered inaccessible.

Additionally, the **industry** in which you operate plays a large role regarding your risk. When it comes to data breaches, the public sector represents the highest rate of risk, with administrative, information, financial, and management sectors following (source: IRIS 20/20 Cyentia, 2021). When it comes to ransomware, Professional Services, Consumer Services, Public Sector, Materials and Healthcare are the most frequent targets (source, Coveware, Q4 2021).

The size of firm matters, as well. Firms with over $1B in revenues have a greater than 12x the probability of a data breach that firms under $10M in revenues have. **But ransomware does not discriminate with regards to size.** The median size firm targeted by ransomware in Q4, 2021 was only 133 employees.

The other factor to deciding coverage is going to be, **how long can you afford to be down** in the event of a cyber-attack. The cost to restore your systems in the case of an event should also be considered.

I typically counsel clients on the smaller side, to look at $1,000,000 in coverage for third- and first-party coverages with $50,000 to $250,000 for fraud coverages. Larger mid-size firms, especially in high-risk categories are going to need upwards of $5M to $10M in coverage. Of course, often the biggest determinate of how much coverage you need is how much your largest customer is demanding you have.

Deductibles, waiting periods, sub-limits, and co-insurance

Carriers use various ways to help manage their risk, including the extent to which businesses have "skin in the game" when it comes to cyber security. **Deductibles** have long been used as a way to have the insured participate in the loss; however, where it was once not unusual to see $1,000 deductibles, expect to see $5,000 or $10,000 deductibles as minimums. When it comes to business income coverage, a **waiting period** or number of hours that a system is down is used instead of (or at least in addition to) a deductible.

Sub-limits are often used to reduce the exposure a carrier has certain coverages. With regards to cyber insurance, it has been used mainly for fraud coverages and increasingly for ransomware.

In addition to, or instead of sub-limits, **Co-insurance** is starting to be added to coverage for higher risk firms to increase the insured's participation in the loss. An example would be a 10% coinsurance in the event of ransomware. If the firm had this coinsurance on a $1M liability policy, they would share 10% of the loss up to $100,000 out-of-pocket. This may seem excessive, but it might be the only way a higher risk firm could secure terms it needs.

What are carriers looking for when placing coverage?

Carriers are looking at several factors. Key components typically start with the size of the firm in revenues, its industry and the quality of the firm based on how long it has been in business, employee turnover and client retention. Like most insurance coverage, loss history is an important factor both in setting pricing as well as whether they will write the firm.

Carriers are also now increasingly looking at what cyber security controls you have in place. There controls include:

> **Multi-Factor Authentication (MFA):** MFA is basically a two-step verification anytime you log in. An example would be a password and then something that comes up on your cell phone.
>
> **End Point Detection and Response (EDR):** EDR helps identify threats at the endpoint -- your laptop or your cell phone or some other external device -- and attempt to lock it down before it infects the rest of your network.
>
> **Patching:** Patching is a process of updating your computer systems when software or firmware updates are provided. Often, they include critical security patches that help protect your system from hackers looking to exploit bugs.

Access Control: Have strong passwords, use a Virtual Private Network (VPN) when accessing your systems remotely and assign rights to your system sparingly. Carriers are concerned about something called Remote Desktop Protocol, which is often used by hackers to get into networks. Make sure it is blocked from the internet or extremely locked-down.

Backups: Carriers are certainly looking to see what you have in terms of your backup protection, and specifically, do you have an offsite backup solution? It is important to note that you should be testing that backup on an ongoing basis to make sure you can recover it when you need to.

Training: Lastly, they are looking to see whether you are employing some type of security awareness program that includes phish simulation training. Over 60% of the risks to the organization come from human risks when it comes to cyber security. So, you want to make sure that your staff is trained properly to deploy the best digital habits that they can.

What happens when there is an incident?

When an organization suffers a cyber security incident, it is important to contact the carrier as soon as possible. Carriers will typically have a panel of law firms, forensic companies, breach coaches and other services to assist the organization protect itself from further harm and get back on its feet as soon as practical. If you have a ransomware attack, they will also help direct you in terms of how to best negotiate, if you are going to negotiate at all, and who to bring into that process. Typically, you want to bring in the FBI or some government agency to help you in in that process as well as technical expertise to help you restore and get your systems up and running as quickly as possible, and preferably without having to pay that ransom.

How are premiums rated?

As mentioned previously, industry and revenues are the beginning data points for pricing on almost every policy. Beyond that, they will look at what security controls you will have in place. The absence of a number of those controls previously mentioned will result in a higher premium, and certainly it may just be the determinant of whether you qualify for coverage at all. The quality of your organization is important because a main component in cyber security is human risk. Loss history is another big factor. A third of organizations that have been hacked over the past 12 to 18 months get hacked again within a relatively short period of time; that is why it is often extremely difficult for firms that have recently been hacked to find coverage.

What happens if something is true when I applied for coverage but is now not true after filing the claim?

It is a great question, and it will depend on the carrier. I will say that if it was true and you answered the application truthfully, carriers typically will stand by the claim. It is the situations in which if it is discovered that you answered a question dishonestly, or if an event was triggered because of a control being in place or not in place that you did not disclose in your application, that you could potentially be without coverage.

What is next for cyber insurance?

Over the past two years, we have seen the pace of digital transformation change faster than ever before. As digital advances continue in Artificial Intelligence, Virtual and Augmented Reality, Healthcare, Crypto and Blockchain (to name a few), both digital risks and the means to protect and finance them will evolve as well. This makes it extremely hard to quantify cyber risk. And this difficulty often results in fluctuating premiums and rapidly changing carrier appetites. Our view is that cyber insurance works best when it has visibility into how prepared the organization is to mitigate cyber risk – that ultimately creates competitive and stable pricing. Expect more coverage advances in response to the new risks as well as ways to protect and continuously monitor cyber risk. After all, it is fair to say that we live in as much a digital as well as an analog world – we need to be able to confidently transfer risk through vehicles like cyber insurance if we are to be successful.

If you would like more information about Cyber Insurance or would like to learn more about SeedPod Cyber, please contact us at info@SeedPodcyber.com